REMARKS

The Examiner has rejected Claims 1-23 under 35 U.S.C. 101 as being directed towards non-statutory subject matter. Applicant respectfully asserts that such rejection is avoided in view of the amendments made hereinabove to independent Claims 1 and 16. Specifically, applicant has amended independent Claims 1 and 16 to include an operating system identification system including "a tangible computer readable medium."

The Examiner has rejected Claims 1-5, 7-9, 11, 12, 16, 17, 19, 20, 39 and 41-44 under 35 U.S.C. 103(a) as being unpatentable over Fyodor ("Remote OS detection via TCP/IP Stack FingerPrinting"), in view of Canis et al. (U.S. Patent Publication No. 2002/0138605). In addition, the Examiner has rejected Claims 14, 15, 22-27, 29, 30, 32-37 and 40 under 35 U.S.C. 103(a) as being unpatentable over Fyodor, in view of Canis, and further in view of Karadimitriou et al. (U.S. Patent No. 6,618,717). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to the independent claims.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the Fyodor and Karadimitriou references, the Examiner has argued that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to use Karadimitriou's confidence level with Fyodor's

tests in order to provide the highest level of probability of an accurate identification as suggested by Karadimitriou." Applicant respectfully disagrees and asserts that it would not have been obvious to combine the teachings of the Fyodor and Karadimitriou references, especially in view of the vast evidence to the contrary.

For example, Fyodor relates to utilizing a fingerprinting technique to determine a host operating system, while Karadimitriou relates to identifying a content owner of a Web site . To simply glean features from a fingerprinting technique, such as that of Fyodor, and combine the same with the *non-analogous art* of identifying a content owner of a Web site, such as that of Karadimitriou, would simply be improper. In particular, a fingerprint technique is used to determine a host operating system (Fyodor – Page 1, Abstract), while identifying the content owner of a Web site involves "collect[ing] candidate names from the subject Web site...[and] run[ning] tests that provide quantitative/statistical evaluation of the candidate name being the content owner name of the subject Web site" (Karadimitriou – Abstract). "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a fingerprint technique addresses as opposed to identifying a content owner of a website, the Examiner's proposed combination is inappropriate.

Thus, applicant respectfully asserts that the first element of the *prima facie* case of obviousness has not been met, since it would be *unobvious* to combine the references, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended the independent claims to further distinguish applicant's claim language from the Fyodor, Canis, and Karadimitriou references, as follows:

"wherein a confidence level is assigned to the identification of the operating system based on a predetermined confidence level stored in association with at least one of a plurality of identification fingerprints used to identify the operating system" (see this or similar, but not necessarily identical language in the independent Claims 1, 16 and 32) and;

"wherein the first confidence level is assigned to the first identification of the operating system, the second confidence level is assigned to the second identification of the operating system, and the third confidence level is assigned to the third identification of the operating system based on a predetermined confidence level stored in association with at least one of a plurality of identification fingerprints used to identify the operating system" (Claim 24).

Applicant respectfully asserts that Karadimitriou teaches that "a probability/confidence level 58 [is] assigned to each candidate name 40," such that "it is straightforward then to choose the candidate name 40 with the highest probability of being the Web site's 42 content owner name" (column 8, lines 46-49 - emphasis added).

However, assigning a probability/confidence level to each candidate name, in addition to choosing the candidate name with the highest probability of being the Web site's content owner name, as in Karadimitriou, fails to suggest a technique "wherein a confidence level is assigned to the identification of the operating system based on a predetermined confidence level stored in association with at least one of a plurality of identification fingerprints used to identify the operating system" (Claims 1, 16 and 32 – emphasis added), and a technique "wherein the first confidence level is assigned to the first identification of the operating system, the second confidence level is assigned to the second identification of the operating system, and the third confidence level is assigned to the third identification of the operating system based on a predetermined confidence level stored in association with at least one of a plurality of identification fingerprints used to identify the operating system" (Claim 24 – emphasis added), as claimed by applicant. Clearly, assigning a probability/confidence level to each candidate name, as in

Karadimitriou, fails to even suggest "assign[ing]...based on <u>a predetermined confidence level</u> stored in association with <u>at least one of a plurality of identification fingerprints</u>" (emphasis added), as claimed by applicant.

In addition, applicant has further amended the independent claims to further distinguish applicant's claim language from the Fyodor, Canis, and Karadimitriou references, as follows:

"wherein the identification of the operating system by one of the operating system identification tests is dependent on the identification of the operating system by another one of the operating system identification tests" (see this or similar, but not necessarily identical language in the independent Claims 1 and 16);

"wherein the first identification of the operating system, the second identification of the operating system, and the third identification of the operating system by one of a plurality of operating system identification tests are dependent on the identification of the operating system by another one of the operating system identification tests" (see Claim 24); and

"wherein the identification of the operating system by one of the plurality of tests is dependent on the identification of the operating system by another one of the plurality of tests" (see Claim 32).

Applicant respectfully asserts that Fyodor teaches that "[t]here are many, many techniques which can be used to fingerprint networking stacks" and that "you just look for <u>things that differ among operating systems</u> and <u>write a probe for the difference</u>," where "[i]f you <u>combine enough of these</u>, you can <u>narrow down the OS very tightly</u>" (Page 4 – emphasis added).

However, fingerprinting network stacks by looking for things that differ among operating systems, writing a probe for the difference, and <u>combining enough of the</u>

probes to narrow down the OS, as in Fyodor, simply fails to even suggest applicant's claimed technique "wherein the identification of the operating system by one of the operating system identification tests is dependent on the identification of the operating system by another one of the operating system identification tests" (Claims 1 and 16 – emphasis added), "wherein the first identification of the operating system, the second identification of the operating system, and the third identification of the operating system by one of a plurality of operating system identification tests are dependent on the identification of the operating system by another one of the operating system identification tests" (see Claim 24 – emphasis added), and "wherein the identification of the operating system by one of the plurality of tests is dependent on the identification of the operating system by another one of the plurality of tests" (see Claim 32 – emphasis added), as claimed by applicant.

Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 30, the Examiner has relied on, in part, Page 11 (partially excerpted below) from the Fyodor reference to make a prior art showing of applicant's claimed technique "wherein generating a list of open ports comprises retrieving a previously constructed list of open ports."

```
"We use the command:
nmap -sS -F -o transmeta.log -v -O www.transmeta.com//24

This says SYN scan for known ports (from/etc/services), log the
results to 'transmeta.log', be verbose about it, do an OS scan,
and scan the class 'C' where www.transmeta.com resides. Here is
the gist of the results:" (Fyodor, Page 11 – emphasis added)
```

Applicant respectfully asserts that Fyodor merely discloses that the nmap command says to SYN scan for known ports from /etc/services and log the results to a log file. However, simply scanning for <u>known ports from /etc/services</u>, as in Fyodor, fails to suggest "retrieving <u>a previously constructed list of **open ports**</u>" (emphasis added), much less a technique "wherein generating a list of open ports comprises retrieving <u>a previously constructed list of **open ports**</u>" (emphasis added), as claimed by applicant.

Again, since at least the first and third elements of the *prima facie* case of obviousness have not been met, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 46-49 below, which are added for full consideration:

"wherein each operating system identification test executed by the identification module causes a first plurality of packets to be transmitted to the network node and a plurality of response packets to be received by each operating system identification test" (see Claim 46);

"wherein the plurality of response packets are reformatted for use in identifying the operating system being executed by the network node" (see Claim 47);

"resolving conflicts among the at least one of the identifications made by the plurality of operating system identification tests only if none of the at least one of the identifications is associated with the confidence level greater than the predetermined confidence level" (see Claim 48); and

"wherein the resolving conflicts is based at least in part on comparing aggregated results from at least two of the plurality of operating system

identification tests with a plurality of conflict resolution definitions" (see Claim 49).

Again, a notice of allowance or a proper prior art showing of <u>all</u> of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P333).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100